OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

Report PH-2016-001

October 31, 2016

Eastern Health

Summary: An intentional privacy breach occurred at Eastern Health when an unknown person inappropriately accessed and printed personal health information from the Meditech account of a doctor at Eastern Health. This information was then anonymously sent to the Department of Health and Community Services and the College of Physicians and Surgeons. It could not be proven who committed the breach, so no charges were laid under section 88 of the *Personal Health Information Act*. The Commissioner found that Eastern Health had taken reasonable administrative and technical security measures to protect personal health information as required by section 15 of *PHIA*. This breach appears to have been outside of Eastern Health's control and perpetrated by someone who chose to ignore clear rules and policies regarding the protection of personal health information. This person was able to inappropriately access the information through the account of another doctor when he inadvertently failed to log out of his computer session, contrary to Eastern Health policy. The Commissioner recommended that Eastern Health review best practices for automatic log out times and implement an appropriate standard consistent with privacy best practices and professional practice requirements. The Commissioner also recommended that Eastern Health remind employees of the importance of logging out of computer sessions and of the consequences for failing to do so.

Statutes Cited: *Personal Health Information Act*, S.N.L. 2008, c.P-7.01 sections 15 and 88.

Authorities Relied On:

Newfoundland and Labrador OIPC Report PH-2013-001 at www.oipc.nl.ca.

File #'s: 0180-060-15-019 and 0180-060-15-021

I BACKGROUND

[1] This Office received two privacy complaints under the *Personal Health Information Act* (*PHIA*) in connection with an intentional privacy breach at Eastern Health that occurred on May 28, 2015 when an unknown person inappropriately accessed and printed personal health information from the Meditech account of a doctor at Eastern Health. This information was then anonymously sent to the Department of Health and Community Services and the College of Physicians and Surgeons. The complainants allege improper use and disclosure of their personal health information as well as inadequate protection of their personal health information. The breach involved more than two patients, but this Report is in response to the two specific complaints received and the health information pertinent to these complainants. The information at issue in these complaints was a Patient Physician Census and consisted of patient names, MCP numbers, sex, age, date of admission to hospital, attending physician and reason for visit.

[2] Despite the thorough investigation undertaken (which included attempted fingerprint/DNA analysis of the envelopes sent to the Department and the College), Eastern Health was unable to confirm, with the necessary degree of certainty, the identity of the person responsible for the intentional inappropriate access. No other avenues of investigation offered any prospect of proving the identity of the offender such that a prosecution would be viable. As a result, this Office determined that pursuing charges under section 88 of *PHIA* was not feasible.

II EASTERN HEALTH'S RESPONSE TO COMPLAINTS

[3] As a custodian, Eastern Health has an obligation to protect the personal health information in its custody in accordance with section 15 of *PHIA.* Inquiries from this Office focused on how this breach happened and whether Eastern Health had reasonable security measures in place to help guard against this inappropriate access. Eastern Health's investigation revealed with certainty what time the records were printed, from whose account they were printed and what printer was used. The records were printed from the

treating physician's Meditech account (an electronic health record system; for more information about the Meditech system, see Report PH-2013-001), however this physician was on rounds in another part of the hospital when the records in question were printed and thus could not have printed them. As such, someone else inappropriately accessed the treating physician's account and printed the information. The treating physician maintains that he did not give his user name or password to anyone else and it appears that the physician did not log out of an active computer session when the clinic finished earlier that morning (the clinic is the location from which the records were printed). The other user accessed and printed the information in question without having to enter their own user name or password.

[4] We have reviewed information sent to us by Eastern Health which included copies of Eastern Health policies clearly setting out acceptable uses of computer resources and specific procedures to be followed by staff to help protect personal health information. Eastern Health also requires that employees, including doctors, complete and sign two forms prior to being issued a computer password and thus given access to the electronic system (the Healthcare Technology and Data Management Form and the CRMS Access Authorization Form). These forms clearly state that the following constitutes a breach of security:

- Disclosure of a password;
- Use of another's password to access the system or information;
- Abuse of authorized access according to the policies and procedures of Eastern Health; and,
- Failure to log off when leaving a terminal or computer.

[5] Confidentiality oaths are sworn (or affirmed) by physicians (and other staff and volunteers) that clearly set out the responsibility to provide for the secure storage of personal health information. The oath also requires acknowledgement that Eastern Health's policy of Privacy and Confidentiality has been read in its entirety and understood.

[6] In addition to the policies and oaths, physicians and other staff are also required to complete orientation upon being hired. Instructions and procedures for use and access of the Meditech system are part of this orientation. Further, through the physician credentialing process of Medical Services at Eastern Health, all new physicians must sign a Confidentiality Pledge (pursuant to Eastern Health's Bylaws Respecting Medical Staff) which specifically addresses breaches and disclosure of personal health information.

[7] In addition to administrative safeguards, the Meditech system is also equipped with several technical safeguards such as passwords and automatic time-outs (i.e. after a specified period of inactivity by the user, the user's session will automatically end). Eastern Health explained that the Patient Care Inquiry menu times out after 1 minute and 30 seconds. The Patient Census menu times out after 6 minutes and 30 seconds. However, they did note that if anyone accesses the open screen at all during the session that the time outs will reset. This could significantly increase the time a session may be left open and could be done inadvertently if a session was left open in the background on a shared computer.

[8] The system on which the information was stored is also password protected. Initial passwords are generated by the system and the end user must then change and set their own password for the system. Passwords must be alpha numeric and current passwords cannot be re-used. Passwords must also be changed every 180 days. Additionally, passwords are stored in Meditech as encrypted data; only system administrators have access to the location of the encrypted data and only the Meditech vendor has the encryption key.

III CONCLUSIONS

[9] It is clear that Eastern Health takes its responsibility to protect personal health information very seriously and has taken care to ensure that administrative measures are in place, including policies and procedures that set out the obligations of all staff and volunteers. All staff are made aware of these obligations. Unfortunately, in this case, it

appears that despite Eastern Health's best efforts to educate doctors, other staff and volunteers, someone chose to inappropriately access personal health information.

[10] The technical measures in place appear to be reasonable, given the realities of the Meditech system, however, review of privacy best practices with respect to automatic log out times is recommended. As an example, the installation of proximity card readers at computer workstations that rapidly and automatically log off a user when the user leaves the workstation would prevent unauthorized access to another user's account. This technology adds another authentication factor. While the technology can be configured differently in different settings, simply explained, it operates by permitting log in (which still requires a password) when the card reader detects the physical proximity of the card and then, perhaps most importantly, automatically logs users out when they leave the workstation (as the card can no longer be read or detected by the card reader). Our preliminary research indicates that this technology can be tailored for multi-user workstations and that user sessions can be quickly restored (even at a different workstation) when the reader enabled workstation detects the return of the authorized user within a configurable grace period. This allows users to "roam" between workstations without having to log in and out every time. This measure, depending on cost, may or may not be "reasonable" but it is worth consideration, as it does not depend on manual log out by the user to protect personal health information, thus addressing one of the major problems of policy enforcement: ensuring consistent end-user compliance.

[11] Secure print systems are another option worthy of consideration as a "reasonable" security measure. Secure print systems require a personalized, unique code to be entered into a printer in order for the print job to be completed. Open printers facilitate conduct that occurred here (as the person who printed the information is unidentifiable) and also heighten the risk of inadvertent breaches.

[12] I conclude, based on the evidence before me, that Eastern Health has taken reasonable administrative and technical security measures to protect personal health information as required by section 15 of *PHIA.* This breach appears to have been outside of Eastern Health's control. Clear rules and policies regarding the protection of personal information

are in place and communicated to all employees and volunteers by various means. In this case an individual deliberately chose to ignore them. Unfortunately, it was impossible to determine with reasonable certainty who committed the breach. It must also be mentioned however, that the breach was one of opportunity; afforded to this person when the treating physician inadvertently failed to log out of his computer session earlier in the day, contrary to Eastern Health policy.

VI RECOMMENDATIONS

[13] Despite finding that the current security measures are reasonable, as with any system, there may be areas that can be improved upon. As such, it is recommended that Eastern Health review best practices for automatic log-out times and implement an appropriate standard consistent with privacy best practices and professional practice requirements. This includes a consideration of proximity card readers for computer log on/off and secure print systems. Eastern Health should also consider whether operational requirements would allow for system defaults within Meditech to be set to preclude a user being simultaneously logged in on different terminals. While reviewing its practices, Eastern Health should also consider the feasibility of routine random "privacy spot checks" to assess end user compliance with policies , particularly with respect to users logging out of computer sessions prior to physically leaving a workstation.

[14] Finally, it is also recommended that Eastern Health remind physicians and other staff about the importance of logging out of the computer system immediately upon completion of the task at hand or as soon as operational/practical requirements allow, and the potential consequence to them if they fail to do so. This point should continue to be made from time to time in privacy training and awareness communications.

[15] Under the authority of section 74(1) of *PHIA*, I direct Eastern Health to write to this Office and the Complainants within 15 days of receiving this Report to advise of its decision regarding the recommendations in this Report.

[16] Dated at St. John's, in the Province of Newfoundland and Labrador, this 31st day of October 2016.

Donovan Molloy, QC
Information and Privacy Commissioner
Newfoundland and Labrador